



FortiClient EMS - Release Notes

Version 1.2.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 07, 2017

FortiClient EMS 1.2.2 Release Notes

04-122-455042-20171107

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
System requirements	5
Endpoint requirements	6
Supported Web Browsers	6
Licensing and installation	6
What's New	7
Redesigned navigation menu	7
New Dashboard	7
Sign custom FortiClient installer	7
FortiSandbox authorization of FortiClient	7
Upgrade	8
Upgrading from previous EMS versions	8
Downgrading to previous versions	8
Resolved Issues	9
Known Issues	11

Change Log

Date	Change Description
2017-11-07	Initial release.

Introduction

FortiClient Enterprise Management Server (EMS) is a system intended to be used to manage installations of FortiClient. It uses the same Endpoint Control protocol introduced in FortiOS 5.0 and enhanced in FortiOS 5.2. Like FortiOS, EMS supports all FortiClient platforms: Microsoft Windows, Mac OS X, Android OS and Apple iOS. FortiClient EMS does not require a Fortinet device. It runs on a Microsoft Windows server. End users with FortiClient installations can use a FortiGate or EMS to manage their installations.

This document provides the following information for FortiClient EMS 1.2.2 build 0443:

- [Introduction on page 5](#)
 - [Supported platforms on page 5](#)
 - [System requirements on page 5](#)
 - [Endpoint requirements on page 6](#)
 - [Supported Web Browsers on page 6](#)
 - [Licensing and installation on page 6](#)
- [What's New on page 7](#)
- [Upgrade on page 8](#)
- [Resolved Issues on page 9](#)
- [Known Issues on page 11](#)

For information about FortiClient EMS, see the *FortiClient EMS 1.2.2 Administration Guide*.

Supported platforms

The EMS server can be installed on the following platforms:

- Microsoft Windows Server 2008 R2 or newer

System requirements

The minimum system requirements are as follows.

- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

Internet access is required during installation. This becomes optional once installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.



You should only install FortiClient EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.

Endpoint requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for Mac OS X
- FortiClient for Android OS
- FortiClient for iOS

The FortiClient version should be 5.4.0 or newer.

FortiClient is supported on multiple Microsoft Windows and Mac OS X platforms. EMS supports all such platforms as endpoints.

Supported Web Browsers

The latest version of the following web browsers can be used to connect remotely to FortiClient EMS 1.2.2 GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Internet Explorer is no longer recommended. Remote access may need to be enabled from the FortiClient EMS GUI.

Licensing and installation

For information on licensing and installing FortiClient EMS, see the *FortiClient EMS 1.2.2 Administration Guide*.

What's New

The core features of the FortiClient EMS 1.2.2 include the following:

Redesigned navigation menu

The left navigation menu has been redesigned to provide easier access to the content pane on the right. The top menu has also been merged into the left navigation menu.

New Dashboard

The new Dashboard includes new chart designs and easier access to information and alerts. Administrators can customize the dashboard by moving widgets around.

Sign custom FortiClient installer

You can now sign FortiClient installers created in FortiClient EMS with your own certificate.

FortiSandbox authorization of FortiClient

FortiClient EMS administrators can configure a FortiSandbox IP address in an endpoint profile. After the configuration is saved, FortiClient EMS attempts to submit an authorization request to, and check if it is authorized with, the configured FortiSandbox. If the FortiSandbox administrator authorizes FortiClient EMS, the authorization status is displayed on the FortiClient EMS GUI. Subsequently, all FortiClient endpoints managed by FortiClient EMS are considered authorized by the same FortiSandbox.

This feature requires FortiSandbox 2.5.0 and FortiClient 5.6.1.

Upgrade

Upgrading from previous EMS versions

FortiClient EMS 1.2.2 supports upgrading from the following EMS versions:

- 1.0.3 and later
- 1.2.0 and later

Downgrading to previous versions

Downgrading FortiClient EMS 1.2.2 to previous EMS versions is not supported.

Resolved Issues

The following issues have been fixed in version 1.2.2.

Bug ID	Description
413273	EMS failed to synced with Domain controller
415238	Add option for user to sign Custom FortiClient installer created by EMS
417253	EMS GUI is not displayed correctly with low screen resolution or small browser window
420969	FortiClient EMS Software Manager strips Code Signing Certificate on customer FortiClient installer
421319	Option to disable "block malicious websites" when on-net
434304	Endpoints Filter by OS and FortiClient Version
434328	ssl3 and tls1.0 cannot be disabled on EMS server
438310	Sidebar Sort domains in alphabetical order
441134	Error when running FCMDaemon --dbg=71 > logfile.txt 2> logfile.err.txt
441704	"Desktop shortcut" and "Start menu shortcut" are not working as expected in the installer
443623	FCMAdDaemon crash
446280	EMS fails to uninstall forticlients on endpoints
447056	Email AV alerts should include action
447352	<dnscache_service_control> tag reverted to 1 after profile save
447635	Application Firewall "All Other Known Applications" overrides all other categories
447802	EMS reporting onnet status wrong
447803	Unable to import FortiClient profiles from 2000E FortiGate
447925	Dashboard summary links don't open for other users except superadmins
448858	EMS report is inconsistent with FortiClient
449894	Forticlient EMS installer package does not appear to be licensed for MAC installs
451370	GUI does not load completely if admin username begins with 3 or more digits
452963	Log upload frequency does not seem to follow configured value for log_upload_freq_minute
454087	Deployment Section suggests "Domain/User" instead of "Domain\User"
455160	FCMAdDaemon crash

Bug ID	Description
456149	Forticlient EMS can't import EC profile which enable webfilter profile and web_url action is exempt

Known Issues

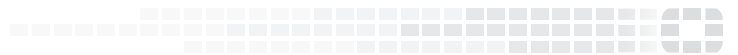
The following issues have been identified in version 1.2.2. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Bug ID	Description
402101	Add option to remove all FortiClients but keep Devices
402842	EMS attempting to login with an account "A" that was never configured on it.
404629	EMS displays domain machines when you click on "Endpoints" but not under a domain
405092	False Positives and Incorrect Use of the Term Zero Day: FortiClient / FortiSandbox integration
409587	Deployment Task does not start
410722	Need a way to lock down EMS Profile when EndPoints managed by different non-Super Administrators
413182	After upgrading to 1.0.4 endpoints not registering properly
413419	FortiClient and EMS server should prevent installation and upgrade to unsupported OS versions
413432	Suggest to add msi installer when creating installers on EMS
413530	Windows still rebooted even though FCT user don't want to reboot it
414620	EMS and OpenDirectory/LDAP
414742	Unable to install EMS server due to Apache crash
415443	Unable to upgrade FortiClient EMS to 1.0.5
415585	Redeployment from EMS will reboot servers as no users logged in
416068	EMS LDAP Authentication - SASL
417285	Inconsistence with EMS and FortiGate registration wording
417288	Different feature icons in profiles, client details and FortiClient Console
433941	Deployed FortiClient has only compliance feature
435538	RealTime Scan Logging / Alerting should show more details
437707	Webfilter cannot enable without enabling FortiProxy
438215	FortiClient EMS slow to load profile

Bug ID	Description
438218	Unable to save profile after adding new applications signatures to customer's application overrides profile
440139	After upgrading the EMS from 1.0.5 to 1.2.1, some vpn settings are lost or don't work as intended
446313	Sometimes FortiClient Endpoints Not Syncing to EMS - Faulting application name: FcmDaemon.exe
447016	Unable to add Domain User To Administration Tab of User Management in EMS 1.2.1
448016	Access to EMS by Group Membership
448080	"Mark as Uninstalled" should be available for offline domain endpoints
448480	Improve unquarantine behaviour
448485	Change onnet/offnet status discovery for dual registration case
451605	EMS reports NPAPI Flash Plugging vulnerable while not installed
454697	Add an option to find where profile is assigned
455188	Unable to open the "Errors or Warnings (last 7 days)" on the EMS when there is a big amount of events
458135	Display FortiClient Serial Number on the EMS GUI



FORTINET®



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.